CYBER SECURITY ASSESSMENT

Identify risks and vulnerabilities in your digital infrastructure

ultima

With an ever-changing threat landscape and advancements in technology, maintaining a strong cyber security strategy is critical. Achieving a balance between dynamic, responsive, accessible systems and a secure, locked down and managed environment is a continual challenge. While the shift from server to service-based infrastructure is transforming how business operations are delivered, it has generated new security concerns which need to be mitigated. Organisations must protect an increasingly mobile and global workforce, alongside cloud-based applications, distributed data and a plethora of both managed and unmanaged devices.

Organisations rarely stand still - instead they continually evolve, often establishing new territories as they expand. Whether it be the increasing number of network entry points requiring protection, or the servers and infrastructure that host vital workloads and critical data, signature-based threat prevention tools need constant updates to remain secure. Unfortunately there isn't a single solution that meets all of these challenges. Instead, IT must engage stakeholders from all parts of the business, combining people and processes with technology controls... in order to deliver effective security policies across the enterprise.

Policy and Best Practice

Ensuring that security policies are aligned to corporate governance and complicit with government legislation is a constant challenge that must be considered. It is a requirement of every business to apply security policies against the huge amount of data that is being created, sent, stored and archived on a daily basis. A lack of understanding of the risks can often result in misaligned security policies.

Centralised Visibility

Organisations are blind to the risks they are facing from outside threats, without instant visibility of their security position. Only when these risks have been identified can remedial action be taken to address issues, and improve the security of the business. Alongside non-compliance; the lack of visibility and understanding causes existing infrastructure to be exposed to cyber attacks.

Vulnerability Management

With the growth and complexity of business applications, systems and infrastructure, identifying and remediating against vulnerabilities can be difficult. This is usually met through a combination of manual processes, outdated methods and an array of vendor products that do not necessarily provide the information needed to maintain a secure environment. Without a comprehensive approach to vulnerability management, systems will remain insecure.

Threat Management

As cyber criminals develop ever more sophisticated threats and tactics, organisations have an obligation to secure their critical data and protect their employees wherever they reside. This involves deploying threat prevention technology within data centre, private or public cloud platforms - and on mobile devices. Signature-based technology that can only prevent against known threats is not adequate, and will not protect against modern "zero day" malware threats.

1

An Average Day in an Enterprise Organisation

Organisations are no longer autonomous entities, air-gapped from the outside world. Instead they have become highly interconnected and increasingly complex - often federating between each other, integrating with third party cloud and application hosting services, and leveraging modern working practices in order to remain competitive. Since the number of possible access and egress points on any given network has increased dramatically, together with the recent explosion of mobile devices and BYOD, IT teams are considering how to continue providing flexible and dynamic services on a daily basis, without relaxing borders and associated security policies.

Given the proliferation of threats, such as phishing, zero day malware, DDOS attacks, bot infiltration and ransomware, companies are looking at employing multi-layer cyber security solutions, in order to provide everything from URL filtering, threat protection and application control, to firewalls, anti-bot / virus / spam and intrusion protection.

Every 81 Seconds
a known malware is downloaded

Every 4 Minutes
a high-risk app is used

Every 53 Seconds
a bot communicates with its command and control

Every 4 Seconds
an unknown malware is downloaded

Every 5 Seconds
a host accesses a malicious website

Every 30 Seconds
a zero day malware event occurs

88% of Companies
suffered a data loss incident in 2015

94% of Companies
used at least one high-risk application

Every 32 Minutes
sensitive data is sent outside the organisation

400% Increase
in the loss of business data since 2013

1/5 Mobile Devices
are infected with some form of malicious code

75% of Businesses
were found to have existing bot infections

Source
Check Point
Software Technologies
Security Report 2016

2

Ultima Cyber Security Assessment

Our Cyber Security Assessment offers an independent security review, helping to identify gaps, and provide recommendations, around areas in which your organisation may be vulnerable to cyber threats. Delivered by our security specialists, the engagement looks at a wide range of attack vectors, providing proactive advice, backed by industry best practice and established accreditations.

Threat Analysis

Our threat analysis tool will provide instant visibility of significant risks to your network, including zero day malware infections, botnet traffic, unauthorised applications and sensitive data leakages. The deep dive findings are presented back and discussed at the infrastructure review stage.

Vulnerability Assessment

The CREST accredited vulnerability assessment will provide a penetration test against the external facing components of your network infrastructure, simulating an attack on your applications, systems, people or facilities. We will help identify weak points in your defences, and streamline the remediation process.

Infrastructure Review

Our experts will work with your team to baseline your infrastructure, and document our findings against industry best practice such as Government 10 Steps to Security, SANS and Cyber Essentials. We will provide a gap analysis of your infrastructure to obtain the Cyber Essentials certification (this is an additional option).

Key Benefits

01

Policy and Best Practice

We will deliver a document containing a list of prioritised recommendations, outlining the changes required to become more secure.

02

Security Visibility

Gain insight into what's happening inside your network, while identifying and understanding the threats you are exposed to.

03

Cyber Essentials

We are able to help you obtain Cyber Essentials certification, in order to demonstrate a level of security control.

04

Vulnerability Awareness

Test the security of your perimeter networks and understand the risk of threats coming from outside your organisation.

3

About Cyber Essentials

The Cyber Essentials scheme is a government-backed cyber security standard, of which organisations can be assessed and certified against. It identifies the security controls that an organisation must have in place within their IT systems, in order to ensure that they are addressing cyber security effectively and mitigating the risk from internet-based threats.

Whilst providing a basic, but essential, level of protection, the scheme enables organisations practicing robust cyber security, to benefit by making this a unique selling point. Cyber Essentials certification will help protect your organisation against common cyber threats, show your customers you take this issue seriously, and enable you to bid for Government contracts.

The scheme focuses on internet-originated attacks, however many organisations will have particular services, e.g. web applications that will require additional and specific controls - beyond those provided by Cyber Essentials. Cyber Essentials requires you to have five technical controls in place.

- Boundary Firewalls
- Secure Configuration
- User Access Control
- Malware Protection
- Patch Management

CYBER ESSENTIALS

About Ultima

Ultima has a proven record of accomplishment in the supply of enterprise security solutions, throughout many diverse and highly complex corporate environments. Focused across two main areas, our Assurance and Compliance business helps identify the threats to your organisation and prioritise your risk treatment, as well as comply with standards such as ISO 27001, General Data Protection Regulation (GDPR) and PCI DSS. Our technology team can help you with the design, implementation and support of networking technologies and security controls.

- Strategic risk-based advice aligned to business objectives
- End-to-end capability embracing all aspects of people, process and technology
- Extensive industry experience with skill-sets across multiple vendor technologies
- Full design, support and managed services
- Top accreditations with leading technology vendors

Certified Experts
Delivered by qualified consultants from our Assurance and Compliance practice, specialising in delivering cyber security engagements.

Hybrid Experience
We have extensive expertise in designing, developing, implementing and managing multi-vendor network and security solutions.

Vision and Leadership
Our architects and consultants are able to support strategic business imperatives and become trusted technology advisors.

Connected Services
Gain access to the Ultima ecosystem, linking in associated strategic and tactical engagements including network, security and beyond.

Head Office
Gainsborough House
Manor Park, Basingstoke Road
Reading, Berkshire, RG2 0NA

ultima

0333 015 8000
enquiries@ultima.com
www.ultima.com